

An Easy Win: Using SIGINT to Learn about New Viruses

Project CAMBERDADA
By [REDACTED], I412 (IAD)
& [REDACTED], V252
(NTOC)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20370301

Overall classification

**TOPSECRET//COMINT//
REL TO USA, AUS, CAN, GBR, NZL**

BRICKTOP (2009)

Tascom

RusComNet

Kaspersky

Rosoboron

export

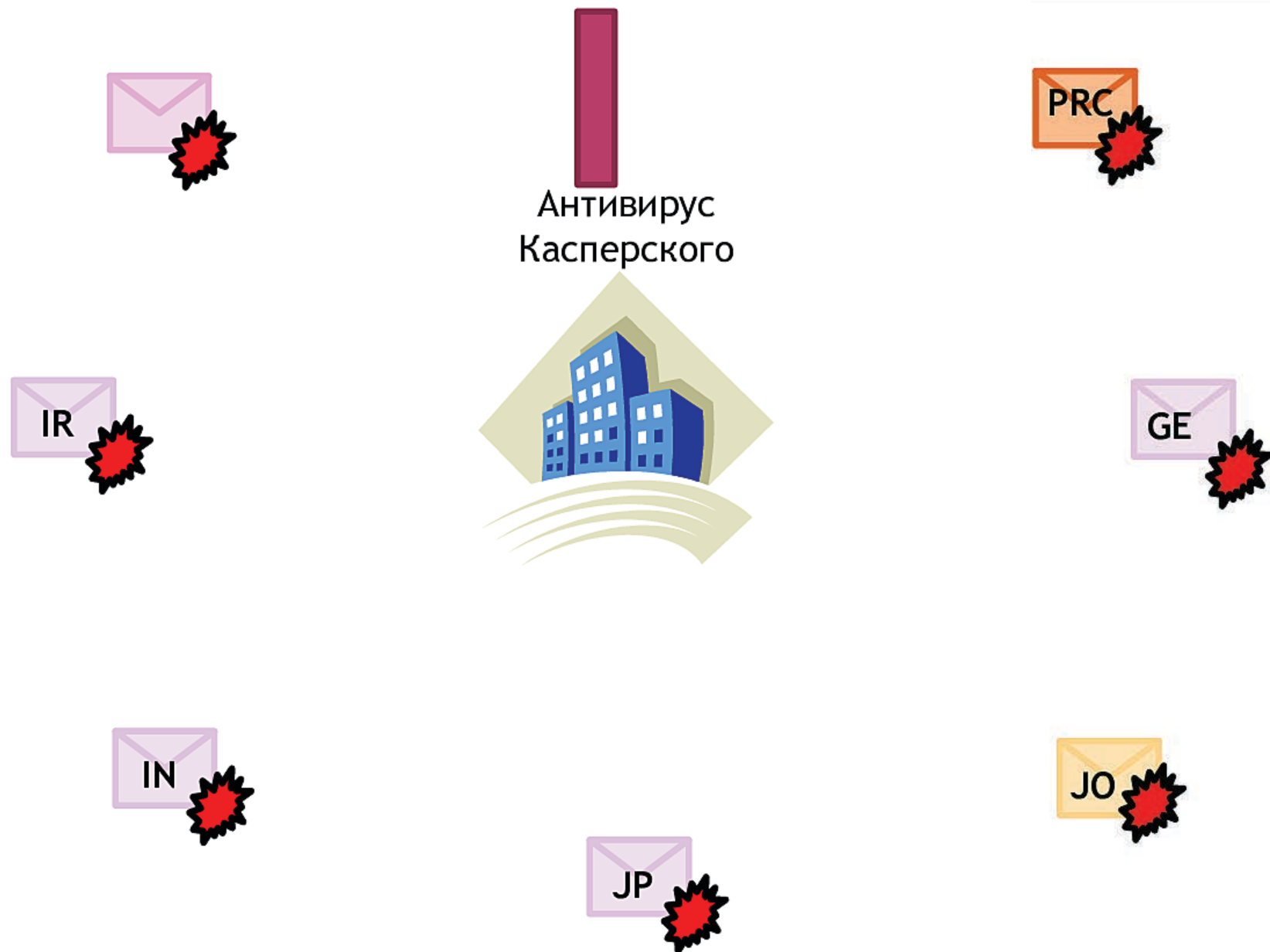
Institute of Information
&
Analytical Technology
(IIAT)

Moscow
Telecommunication
Corporation
(ComCor)

Famatech

Comstar

Komet



Sample Email Received by an AV Vendor

PWZA20120510218350000197506

Good day,

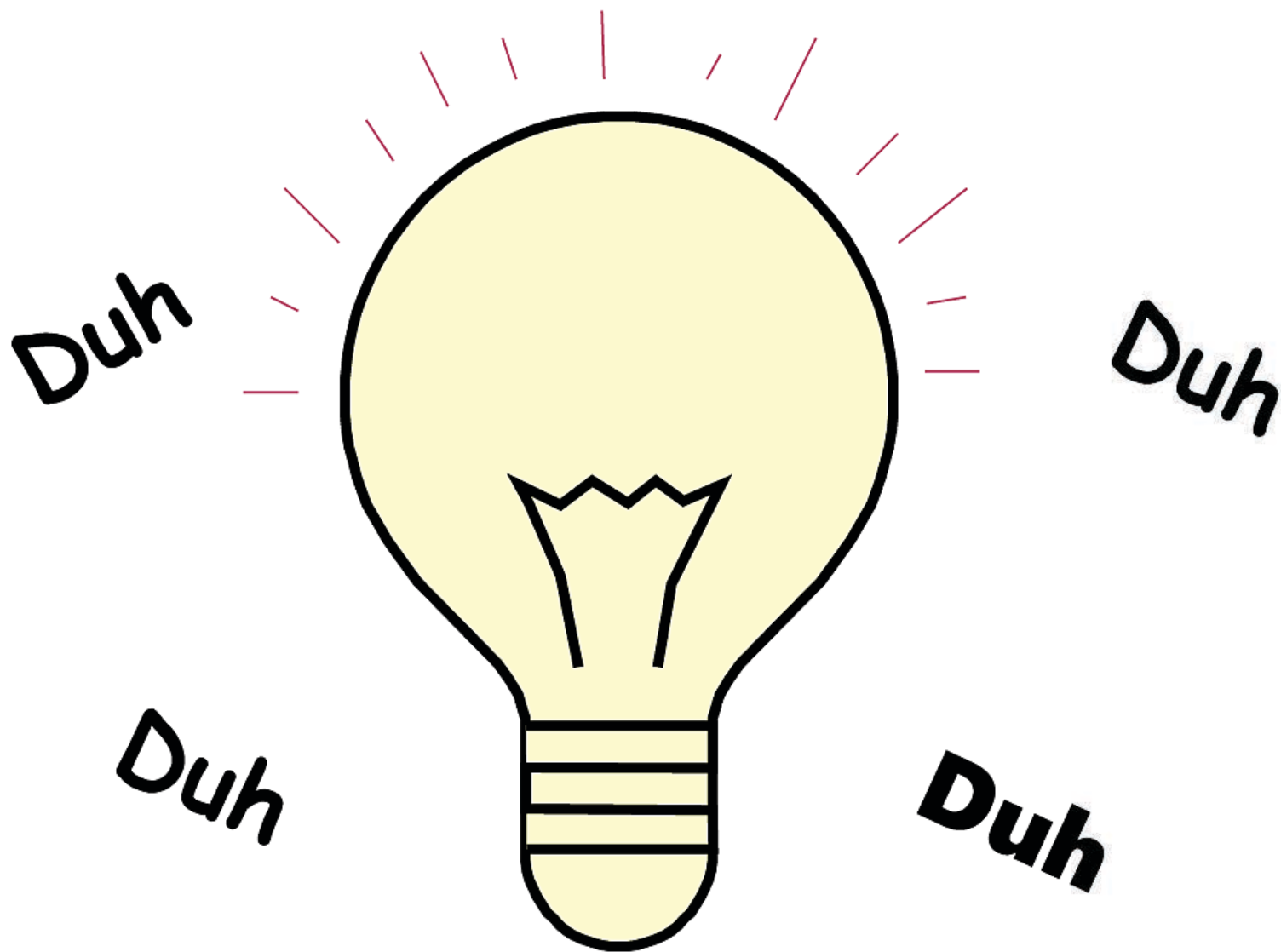
A phishing scam file is attached for your analysis.
Zip file password = **virus**

The file tricks the user into giving her/his bank account credentials. This can be verified by clicking on the *Sign In* button.

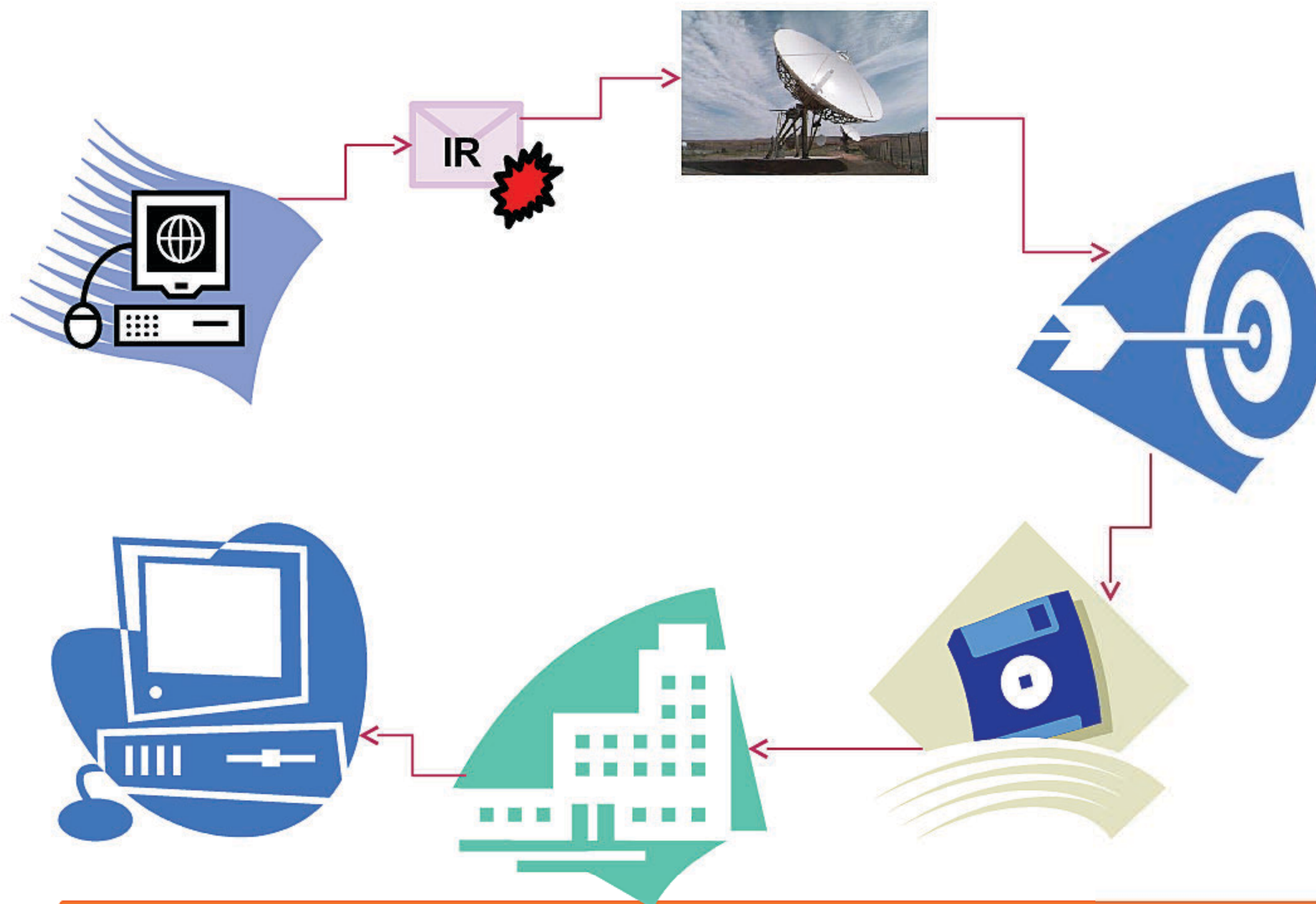
FYI: <https://www.virustotal.com/file/8fb6447fdc9cfe204cde...>

Regards,
Francois Picard
www.NewRoma.net

Attachment: BMOFinancialGroup.zip



Work Flow



Analytic value

孿 SIGINT brings in ~10 potentially malicious files per day for malware triage

孿 Over 500 potentially malicious files collected since 2009

孿 ~ 50 CAMBERDADA signatures deployed to NIPRnet for alerting

孿 9 domains mitigated

DNS Interdiction

- 9 domains under DNS Interdiction

- Cloudshield intercepts the DNS request

- Returns the address of a DoD listening post

- Munged version of the request is sent out

- DNS response is sent to a log

Current status

婦 CRN

- SSO
- Overhead
- SCS
- FORNSAT

婦 IN L-C-2010-147 - Multi-Country: Computer Network Ops

婦 Dozens of CADENCE selectors

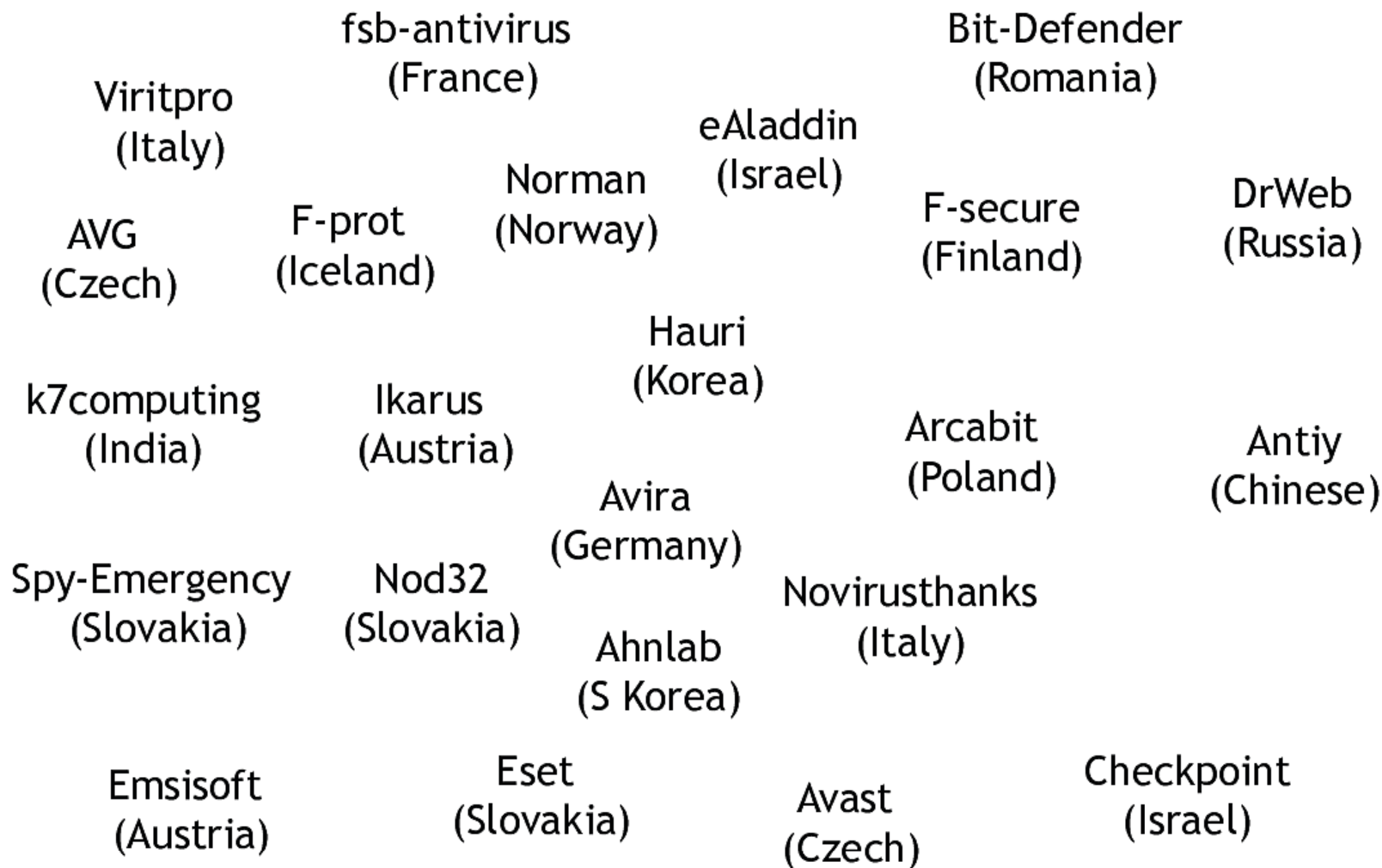
婦 PINWALE daily queries; EXIT4 models

婦 MAILORDER

What else can we do?

- TAO can repurpose the malware
- Check Kaspersky AV to see if they continue to let any of these virus files through their Anti-Virus product
- Monitor the folks who provide the malware to see if they're into more nefarious activity
- Establish automated reporting

More Targets!



A word cloud of antivirus products and their countries of origin. The products are arranged in a roughly circular pattern. The countries are listed in parentheses below the product names. The products are: Viritpro (Italy), AVG (Czech), k7computing (India), Spy-Emergency (Slovakia), Emsisoft (Austria), fsb-antivirus (France), F-prot (Iceland), Ikarus (Austria), Nod32 (Slovakia), Eset (Slovakia), Norman (Norway), Hauri (Korea), Avira (Germany), Ahnlab (S Korea), eAladdin (Israel), Arcabit (Poland), Novirusthanks (Italy), Avast (Czech), Bit-Defender (Romania), F-secure (Finland), DrWeb (Russia), and Antiy (Chinese).

Viritpro
(Italy)

AVG
(Czech)

k7computing
(India)

Spy-Emergency
(Slovakia)

Emsisoft
(Austria)

fsb-antivirus
(France)

F-prot
(Iceland)

Ikarus
(Austria)

Nod32
(Slovakia)

Eset
(Slovakia)

Norman
(Norway)

Hauri
(Korea)

Avira
(Germany)

Ahnlab
(S Korea)

eAladdin
(Israel)

Arcabit
(Poland)

Novirusthanks
(Italy)

Avast
(Czech)

Bit-Defender
(Romania)

F-secure
(Finland)

DrWeb
(Russia)

Antiy
(Chinese)

Checkpoint
(Israel)

T
H
A
N
K

Y
O
U
!

[REDACTED]
I4121
[REDACTED]

[REDACTED]
V252
[REDACTED]

[REDACTED] (S)

[REDACTED] (S)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20370301